

SECRET

US REGISTRY

10 JUL 1987

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Control and Accountability of Removable
Magnetic Storage Media

FROM: Director of Security

EXTENSION

NO.

OS 7 6001

DATE

15 MAY 1987

DDA/REG
LOGGED

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S
INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. DDA/EXA
7D24 HQS

15 MAY 1987

5/2

JA

2. ADDA

20 MAY 1987

JA

3. DDA

21 MAY 1987

08 JUL 1987

WD

4. ↓

5. D/OS

6.

7.

8.

9.

10.

11.

12.

13.

14. Regraded Unclassified when
Separated from SECRET Attachment

15.

3 to 5: I have held this paper pending the formation of your new Comp Sec group. Now, I believe that Group should formulate a HN for my signature on this topic.

I think the ③ marked elements in attachment should be accomplished soonest. I think all diskettes should be barred from being taken out of the building once in without specific screening. Why have levels. Just say no !!

SECRET

15 MAY 1987

MEMORANDUM FOR: Deputy Director for Administration

FROM: [REDACTED]
Director of Security

SUBJECT: Control and Accountability of Removable
Magnetic Storage Media [REDACTED]


1. This memorandum and the attached background information bring to your attention an information management concern that requires attention. I am referring to the explosion in the use of easily transportable magnetic storage media. Floppy diskettes and other media have inundated our office work environment with the proliferation of PCs and office automation. Development and implementation of an effective information management system for magnetic media will be essential in the maintenance of good security. [REDACTED]

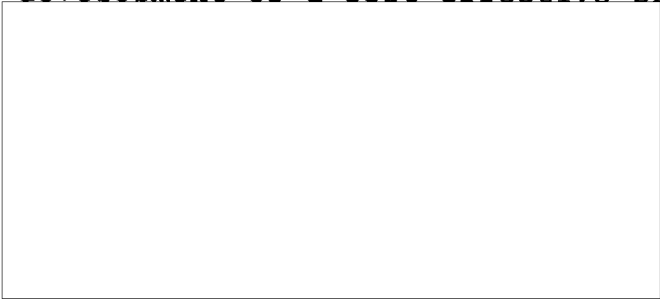
2. I am attaching a white paper that summarizes the problem, what is currently being done to address our concerns, and what needs to be considered for a more effective, long-term solution. While the Office of Security is taking steps to alert personnel at all Agency levels of this growing problem through our education and awareness program, a solution that fully addresses all facets of the problem must be developed and implemented. [REDACTED]

3. Recently, OIS created an Electronic Information Control Task Force to review the bidding on managing and controlling electronic information. Conversations between [REDACTED] Chairman of the Task Force, and [REDACTED] Chief, Information Systems Security Division, indicated that the scope of the task force did not include examining the control and accountability of removable magnetic storage media. This task force's primary focus was to make recommendations pertaining to

~~SECRET~~

S E C R E T

25X1 the policy and procedures required to properly classify different types of records and identify the process for scheduling, archiving, and disposing of electronic records. 

25X1 4. I believe that a task force similar to that created by OIS is needed to examine the issue of accountability of removable magnetic storage media. As an information management concern to this Agency and its senior officials, it is recommended that you give consideration to establishing a similar task force to address controlling removable magnetic media. The task force would examine alternatives and make recommendations for the development of a cost-effective program to solve this problem. 

Attachment

S E C R E T

S E C R E T

WHITE PAPER

25X1 SUBJECT: Proposal for an Agency PC Media Accountability and Control System. []

1. Purpose.

25X1 This paper has been prepared to alert management of the growing security problem with respect to the accountability and control of PC magnetic media. This paper describes the problem and activities currently under way to reduce the problem, and proposes the development and implementation of a PC Media Accountability and Control System (PCMACS) to further solve the problem. We suggest that this proposal be given prompt attention and be taken under consideration by the Deputy Director of Administration for approval. []

2. The Problem.

25X1 A. PC diskettes, currently used within the Agency, have the capability of storing large amounts of information. For example, a 1.2-megabyte floppy diskette may contain 250 fully-packed pages of information (i.e., 60 single-spaced lines of 80 characters each per page) []

25X1 [] Other PC magnetic media used by the PC/AT is capable of containing far greater amounts of information. For example, a removable 20-Megabyte hard disk (a unit of less than 8.14 cubic inches in size) may contain 16.6 books of 250 pages each. []

25X1 B. The Office of Logistics has advised us that their supply store currently distributes an average of five-thousand diskettes per month. These are only 360-Kilobyte diskettes but cumulatively equal 1500, 250 page books per month. Note: Additional 1.2-Megabyte diskettes are obtained through other sources by the Agency. There are indications that, in the not-to-distant future, 5-Gigabyte (five-billion byte) laser disks will be available -- equivalent to two mainframe direct storage devices. []

25X1 C. Currently, the Agency has no system to account for PC magnetic media. Without such a system, the risk of loss or theft of large amounts of sensitive or classified information is increased as is the inability to track or determine the scope of such loss or theft. This risk will further increase

[]

S E C R E T

S E C R E T

25X1 as more magnetic media enters our work environment. Added to this problem, is the fact that many users are not aware of management's concern for the control of PC magnetic media.

3. Current Solutions.

The Office of Security has taken steps to alert Agency personnel about this growing problem and to provide guidelines to reduce this problem. These steps are as follows:

- 25X1 a. Present numerous computer security briefings. These briefings are provided as part of Agency training courses such as Basic VM, GIMS, and OTE courses. Additionally, ISSD/OS has initiated special computer security awareness briefings for each Directorate to alert Agency personnel of our ADP concerns which include the control of magnetic media.
- 25X1 b. Published and distributed the booklet "Security Procedures for Personal Computers" and a reference card "PC User's Quick Reference Security Guide." These documents outline PC media security requirements.
- 25X1 c. Published which requires the use of colored classification labels for all PC media.
- 25X1 d. Provided instructions for the use of Form 4261, to account for the removal of magnetic media from Agency facilities.
- 25X1 e. Prepared and coordinating a Headquarters Notice about the sanitization and destruction of magnetic media.
- 25X1 f. Tested a hardware-based Microcomputer Security System (MCSS) for proposed implementation within the Agency. The MCSS enforces access controls and provided DES encryption of information stored on PC magnetic media.

25X1 Although all of the above items provide, or will provide, increased security, there continues to be a need for a centralized PC media accountability and control system to account for the use of PC magnetic media within the Agency.

S E C R E T

S E C R E T

4. Recommended Solution.

We recommend the development and implementation of a "PC Media Accountability and Control System" (PCMACS). We suggest that the PCMACS be developed to include the following elements:

- 25X1 a. Designate a central procurement authority for all Agency PC magnetic media. ☐
- 25X1 b. Procure only specially-colored diskettes to assure that only Agency diskettes are used in our facilities. Note: This is currently a U.S. Marine Corps policy that is apparently effective. ☐
- 25X1 c. Develop an automated system to account for the procurement and dissemination of all Agency PC magnetic media. ☐
- 25X1 d. Assign all Agency PC media unique ID numbers (e.g., bar codes). There are existing systems on the market that could be used by the Agency. Vendors have demonstrated such systems to the Agency. ☐
- 25X1 e. Assign and authorize only specific component representatives the authority for obtaining media from the central procurement authority. ☐
- 25X1 f. Assign each such representative with the responsibility for: (1) issuance of the media within the component, (2) maintenance of accurate accounting records, and (3) performance of quarterly component audits to account for the issuance, use, and final disposition or disposal of all PC media. ☐

25X1 Note: Implementation of the above described PCMACS will require the involvement and cooperation of several DDA components including the Office of Information Services. ☐

S E C R E T